REMARKS/ARGUMENTS

This Amendment is in response to the Office Action dated January 14, 2004. Claims 1-16 are pending. Claims 1-16 are rejected. Claims 1, 7-9, and 15-16 have been amended. No claims have been canceled. Accordingly, claims 1-16 remain pending in the present application.

Claims 1-2 and 6

Claims 1-2 and 6 are rejected under 35 USC 102(b) as being anticipated by Lessin et al. (4,868,376). The Examiner states:

> Referring to claim 1, Lessin et al. disclose a method for providing a secure transaction, comprising the steps of:
> (a) receiving a new identification (i.e. new PIN) verification data by a transaction device (10) (i.e. a programmable intelligent transaction card) directly from a user (i.e. note process of programming new PIN) (col. 13 lines 20-43);
> (b) storing the new identification verification data on the transaction device only, wherein the new identification verification data is not shared with another device (col. 13 lines 44-48; see Figures 1A and 15C);
> (c) receiving an input of an identification verification data by the transaction device directly from the user (i.e. user uses new PIN) (col. 5 lines 15-24);
> (d) activating the transaction device if the inputted identification verification data matches the new identification verification data (col. 10 lines 2-5; see Figure 11); and
> (e) deactivating the transaction device when an event occurs (i.e. routine exited) (col. 8 lines 27-38)...

Applicant respectfully disagrees as to the claims as amended. In accordance with the present invention as recited in amended independent claim 1, the identification verification data is for the purpose of activating the transaction device, not for the facilitation of the secure transaction. When the input of the identification verification data is received, the transaction device is in a deactivated state. It is not until the inputted identification verification data matches the new identification verification data that the transaction device is activated.

In contrast, Lessin discloses a PIN for the purpose of facilitating a transaction. The transaction device itself is not deactivated. In Lessin, if the incorrect PIN is entered for a particular application, the transaction device can still perform its other functions.

Thus, Lessin does not teach or suggest the combination of steps of recited in amended independent claim 1.

Claims 9-10 and 12-14

Claims 9-10 and 12-14 are rejected under 35 USC 103(a) as being unpatentable over Wallerstein (5,585,787) in view of Mears (5,539,400). The Examiner states:

> Referring to claim 9, Wallerstein discloses a transaction device, comprising: an inputting means (52) (i.e. a keyboard controller circuit) for receiving an inputted identification verification data (i.e. identification number) (col. 6 lines 7-8); a processor (40) (i.e. central processing unit) coupled to the decoder (i.e. a decoder is built-in of a CPU), wherein the decoder asserts an activation signal to the processor (40) if the identification verification data is verified, wherein the decoder de-asserts the activation signal when an event occurs (col. 6 lines 9-28; see Figure 4). However, Wallerstein did not explicitly disclose a decoder coupled to the inputting means for sensing, decoding, and verifying the inputted identification verification data.
>
> In the same field of endeavor of decoding device, Mears discloses a decoder (90) (i.e. an encoder logic) coupled to the inputting means (52) (i.e. keypad array) for sensing, decoding, and verifying the inputted identification verification data (col. 4 lines 9-19; see Figures 1-2 and 4) in order to analyze the keypad array input logic when one of the sensor circuit detect a depressed key.
>
> Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to include an encoder logic coupled to the keypad array for sensing, detecting, and verifying a depressed key disclosed by Mears between the input control and a CPU of Wallerstein with the motivation for doing so would allow faster for the CPU to process and more reliable in order to improve transaction device operate efficiently.
>
> Referring to claim 10, Wallerstein in view of Mears disclose the device of claim 9. Wallerstin discloses wherein the event comprises a completion of a secure transaction (col. 3 lines 1-19; see Figure 5)...

Applicant respectfully disagrees as to the claims as amended. In accordance with the present invention as recited in amended independent claim 9, the decoder of the transaction device senses, decodes, and verifies the inputted identification verification data, where the inputted identification verification data is not shared with another device.

In contrast, the programmable credit card disclosed by Wallerstein temporarily preserves the identification number and completed account number by emulating the numbers on an inducer

behind a magnetic strip provided on the card, and the numbers are subsequently read out from the magnetic strip by a reader device in the form of a conventional magnetic reader. (Col. 3, lines 20-25). Thus, the identification number in Wallerstein is shared with another device, i.e. the reader device.

Therefore, even if Mears teaches the limitations as argued by the Examiner, Wallerstein in view of Mears still does not teach or suggest a decoder for sensing, decoding, and verifying the inputted identification verification data, wherein the inputted identification verification data is not shared with another device, in combination with the other elements as recited in amended independent claim 9.

Claims 3-4 and 7

Claims 3-4 and 7 are rejected under 35 USC 103(a) as being unpatentable over Lessin in view of Grant (6,095,416). The Examiner states:

> ...Referring to claim 7, Lessin et al. disclose a method for providing a secure transaction, comprising the steps of:
> (a) receiving an initial identification verification data by the transaction device directly from the user (i.e. step 860);
> (b) verifying the initial identification verification data by the transaction device (i.e. step 862);
> (c) receiving a new identification verification data by the transaction device directly from the user (i.e. step 878) (col. 13 lines 20-48; see Figure 15C);
> (d) storing the new identification verification data on the transaction device only, wherein the new identification verification data is not shared with another device (col. 3 lines 7-27 and col. 13 lines 20-48; see Figures 1A and 15C);
> (e) receiving an input of an identification verification data by the transaction device directly from the user (col. 5 lines 15-24);
> (f) determining if the inputted identification verification data matches the new identification verification data by the transaction device (col. 5 lines 15-24);
> (g) activating the transaction device if the inputted identification verification data matches the new identification verification data (col. 5 lines 15-24).
>
> However, Lessin et al did not explicitly disclose step:
> (h) starting a timer if the transaction device is activated, wherein the timer expires after a predetermined period of time; and
> (i) deactivating the transaction device when the timer expires.

In the same field of endeavor of method and device of preventing unauthorized use of credit cards, Grant et al. disclose steps:
(h) starting a timer if the transaction device is activated, wherein the timer expires after a predetermined period of time; and
(i) deactivating the transaction device when the timer expires (col. 3 lines 59-62) in order to disable the transaction after a predetermined limited of time so that it cannot be used for a fraudulent transaction.

Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to include steps: starting a timer if the transaction device is activated, wherein the timer expires after a predetermined period of time; and deactivating the transaction device when the timer expires of credit cards method and system disclosed by Grant et al. into portable interactive personal data system of Lessin et al. with the motivation for doing so would allow the transaction to deactivate after a predetermined limited of time to prevent fraudulent transaction.

Applicant respectfully disagrees as to the claims as amended. Applicant's arguments concerning Lessin as applied to claim 1 applies to the rejection of amended independent claim 7 with equal force. For the sake of brevity, these arguments will not be repeated here.

In addition, Applicant disagrees that one of ordinary skill in the art at the time the invention was made would be motivated to combine Lessin and Grant. A feature of the present invention as recited in independent claim 7 is that fact that the new identification verification data is not shared with another device. It is this lack of sharing that limits the fraudulent use of the transaction device.

However, Grant teaches an authorization card that uses a PIN that is shared with another device. The PIN in Grant is a permanent part of the card, and thus the PIN is shared with the manufacturer and whatever device is used to manufacture the device. More specifically, in the magnetic card embodiment, Grant teaches that the PIN code is encoded by cutting the yoke 28 in selected areas to form yoke segments 29 aligned with number or letter positions under a key pad. (Col. 5, lines 40-43) In the electronic card embodiment, Grant teaches that the card is encoded by enabling circuits associated with the PIN code keys by burning out fusible connections 104 to ground. (Col. 10, lines 1-3) In the passive electronic device embodiment, Grant teaches that a variable capacitor 206, and a resonant circuit 200, is provided for each PIN number. (Col. 10, lines

64-65) Since Grant teaches away from an identification verification data that is not shared with another device, one of ordinary skill in the art at the time of the invention would not be motivated to combine it with Lessin to reach the present invention as recited in claim 7.

Thus, Lessin in view of Grant does not teach or suggest the combination of steps of the present invention as recited in amended independent claim 7.

Claim 5

Claim 5 is rejected under 35 USC 103(a) as being unpatentable over Lessin in view of Herwig.

Applicant respectfully disagrees. Applicant submits that claim 5 is patentable when read in combination with its corresponding independent claim 1. Thus, Applicant's arguments above concerning Lessin as applied to claim 1 applies here with equal force. Even if Herwig teaches the limitations as argued by the Examiner, Lessin in view of Herwig still does not teach or suggest the elements as recited in the combination of claims 1 and 5.

Claim 8

Claim 8 is rejected under 35 USC 103(a) as being unpatentable over Lessin et al in view of Grant and in further view of Herwig. The Examiner states

> Referring to claim 8, Lessin et al. in view of Grant et al. and Herwig disclose a method of claim 5 and 7, as evident by claim 8 being equivalent to that the combine of claim 5 and claim 7 "steps a-g" addressed above, incorporated herein. Therefore, claim 8 is rejected for the same reasons given with respect of claims 5 and 7 "steps a-g" combined.

Applicant respectfully disagrees for the same reasons as set forth in Applicant's arguments for claims 5 and 7. These arguments apply here with equal force, and for the sake of brevity, will not repeated here. For these reasons, Lessin in view of Grant and further in view of Herwig does not teach or suggest the combination of steps as recited in amended independent claim 8.

Claim 11

Claim 11 is rejected under 35 USC 103(a) as being unpatentable over Wallerstein in view of Mears and in further view of Suzuki (4,801,787). The Examiner states:

> Referring to claim 11, Wallerstein in view of Mears disclose the device of claim 9. However, Wallerstein in view of Mears did not explicitly disclose further comprising:
>
> a timer circuit coupled to the decoder, wherein the timer circuit is initiated when the decoder asserts the activation signal, wherein the timer circuit expires after a predetermined period of time, wherein the event comprises the expiration of the timer circuit, wherein the decode de-asserts the activation signal to the processor when the timer circuit expires.
>
> In the same field of endeavor of IC card identification system, Suzuki teaches a timer circuit (21T) (i.e. a timer circuit) coupled to the decoder (31) (i.e. a comparator), wherein the timer circuit is initiated when the decoder asserts the activation signal, wherein the timer circuit expires after a predetermined period of time, wherein the event comprises the expiration of the timer circuit, wherein the decoder de-asserts the activation signal to the processor (21) (i.e. CPU within system control section) when the timer circuit expires (col. 2 lines 19-29, 51-56 and col. 4 lines 3-10; see Figures 2 and 3) in order to prevent a fraudulent transaction.
>
> Therefore, it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to include a timer circuit coupled to the decoder, wherein the timer circuit is initiated when the decoder asserts the activation signal, wherein the timer circuit expires after a predetermined period of time, wherein the event comprises the expiration of the tier circuit, wherein the decoder de-asserts the activation signal to the processor when the timer circuit expires of IC card identification system disclosed by Suzuki into transaction system of Wallerstein in view of Mears with the motivation for doing so would allow the transaction to deactivate after a predetermined limited of time to prevent a fraudulent transaction.

Applicant respectfully disagrees. Applicant submits that claim 11 is patentable when read in combination with its corresponding independent claim 9. When read in combination, the timer circuit is initiated when the decoder asserts the activation signal, where the activation signal is asserted when the identification verification data is verified. Thus, the timer circuit defines the period of time during which the transaction device is active.

In contrast, Suzuki discloses a timer circuit 21 which defines the period of time during which a user can enter his identification information, not the time during which the device is

active. With the present invention, the timer circuit is not activated until after the identification verification data has been inputted and verified.

Thus, Wallerstein in view of Mears and in further view of Suzuki does not teach or suggest the timer circuit initiated when the decoder asserts the activation signal, where the decoder asserts the activation signal to the processor if the identification verification data is verified, as recited in the combination of claim 9 and 11.

Claims 15-16

Claims 15-16 are rejected under 35 USC 103(a) as being unpatentable over Mears in view of Wallerstein and further in view of Suzuki.

Applicant respectfully disagrees. Applicant's arguments concerning Mears and Wallerstein and Suzuki as applied to claims 9 and 11 above apply here with equal force. For the sake of brevity, these arguments are not repeated here. Thus, Applicant submits that Mears in view of Wallerstein and further in view of Suzuki does not teach or suggest the combination of elements as recited in amended independent claims 15 and 16.

Conclusion

Therefore, for the above identified reasons, the present invention as recited in independent claims 1, 7, 8, 9, 15, and 16 is neither taught nor suggested by the cited references. Applicant further submits that claims 2-6 and 10-14 are also allowable because they depend on the above allowable base claims.

In view of the foregoing, Applicant submits that claims 1-16 are patentable over the cited references. Applicant, therefore, respectfully requests reconsideration and allowance of the claims as now presented.

The prior art made of record and not relied upon has been reviewed and does not appear to be any more relevant than the applied references.

Applicants' attorney believes this application in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted,
SAWYER LAW GROUP LLP

March 31, 2004
Date

Michele Liu
Attorney for Applicant(s)
Reg. No. 44,875
(650) 493-4540